Universal payment coding system for bank

Patent number: CN1235317
Publication date: 1999-11-17

Inventor: WANG ZIZHONG (CN); GUAN MEI (CN)
Applicant: WANG ZIZHONG (CN)

Classification:
- international: ***G06K9/00; G06K19/067;*** **G06K9/00; G06K19/067;** (IPC1-7): G06K9/00; G06F17/60; G06K19/067
- european:
Application number: CN19990107777 19990531
Priority number(s): CN19990107777 19990531

Abstract of **CN1235317**

A payments cipher system universal to all banks in the same city features that payment encrypting machine authorized by the general headquarter of the People's bank of China is used in conjunction with both private and public keys. It is composed of of the distribution and management system for certificates authorized by the general headquarter, the management system for certificates authorized by city headquarter, the management system for branch banks in a city and the payment decrypting machine for user. Its advantages are high speed and safety and easy operation.

[19]中华人民共和国国家知识产权局

[51]Int. Cl[6]
G06K 9/00
G06F 17/60 G06K 19/067

[12]发明专利申请公开说明书

[21]申请号 99107777.6

[43]公开日 1999年11月17日

[11]公开号 CN 1235317A

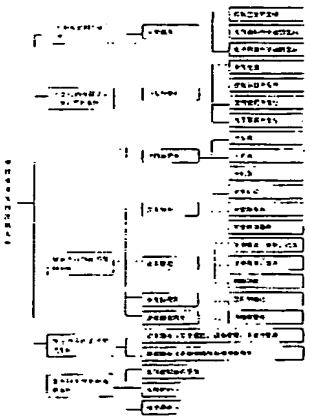
[22]申请日 99.5.31 [21]申请号 99107777.6
[71]申请人 王子忠
地址 100086北京市海淀区北三环西路62号京坤写字楼205号
共同申请人 关 梅
[72]发明人 王子忠 关 梅
[74]专利代理机构 小龙专利代理事务所
代理人 容教璋

权利要求书2页 说明书10页 附图页数7页

[54]发明名称 银行通用支付密码系统

[57]摘要

本发明涉及一种同城市银行通用支付密码系统，解决了现有支付密码应用中存 在的安全性不够、使用不便等问题。本系统使用人民银行总行统一授权认证的 支付密码座机、采用单钥、公钥并用体制，其组成为：人民银行总行的授权认 证卡发行管理系统、城市人民银行的证书管理系统、银行网点的证书管理系统 、客户的支付密码座机系统。使用本系统，可加快资金结算速度和解决票据资 金的安全问题，并可顺利向金融行业资金清算无纸化过渡。



ISSN1008-4274

专利文献出版社出版

99.05.31

权 利 要 求 书

1、银行通用支付密码系统，包括金融网络系统、清算软件系统、支付密码座机以及与支付密码座机配合使用的若干种 IC 卡，其特征在于，所述支付密码座机包括显示、键盘、IC 卡读写接口、通讯接口、打印接口，所述 IC 卡是授权认证卡、支付密码卡和电子票据卡，这三种卡使用时与支付密码座机插接，

授权认证卡是人总行配发的用于对支付者身份及支付行为的基本结算要素进行认证、并控制支付密码座机使用的 IC 卡，

支付密码卡是客户用于为票据签字、并具有计算功能的 IC 卡，

电子票据卡是存放签发好的电子票据的 IC 卡，

本系统的组成包括以下几部分：

1）行业根密钥生成系统，由人民银行总行内部指定专人秘密完成，下级密钥由上级密钥离散生成，

2）人总行的授权认证卡发行管理系统，包括安全服务、卡发行管理、卡档案管理三部分，它的安全服务模块调用密钥生成算法产生人行授权主密钥，把人行授权主密钥和支付密码卡卡号传给子密钥计算函数，产生支付密码卡认证子密钥，再把授权认证卡主密钥和电子票据卡卡号传给子密钥计算函数，产生电子票据卡认证子密钥，授权主密钥、认证子密钥采用单钥密码方案，它的卡发行管理模块调用卡号生成函数生成各种卡的卡号，并将授权认证卡、支付密码卡和电子票据卡分发给城市人行清算中心。它的卡档案管理模块将卡分类管理，可查询统计发卡情况，识别卡的真伪、授权日期、有效期、使用地域等，

3）城市人行的证书管理系统，包括安全服务、证书管理、卡发行管理、和票据接收服务程序，它的安全服务模块采用公钥密码体制，RSA 密码方案，约定人总行、银行网点、客户只拥有一对自己的公钥密钥对，公开钥用于验证签名，秘密钥用于签名。它的证书管理包括证书的申请、更新、挂失、复效、重发及查询、统计等辅助功能，它的卡发行管理对卡进行应用初始化，即建立应用卡结构、写应用基本信息，并进行卡档案管理，它的票据接收服务程序负责处理客户开具的电子票据从支付密码座机拨号到城市人行清算中心的接收工作，

4）银行网点的证书管理系统，包括安全服务、证书管理和票据接收，它的安全服务模块，其算法由一块插在计算机中的硬件加密卡实现，它内置 RSA 密码技术，产生网点及客户的密钥对，对通讯包加密/解密，对证书申请信息和清算信息进行签字/验证，它的证书管理包括证书的申请、更新、挂失、复效、重发及查询、统计等辅助功能，它的票据接收包括支付密码座机和票据接收程序，支付密码座机带有授权认证卡，与电子票据卡互相认证，校验电子票据卡口令，选取票据，处理票据接收程序返回的清算结果回执，

5）客户的支付密码座机系统，包括支付密码座机、支付密码卡和电子票据卡，它的支付密码座机是配合授权认证卡使用、用于签发和验收电子票据卡的终端设备。

2、根据权利要求 1 所述的银行通用支付密码系统，其特征在于，所述授权认证卡中基本信息有：用于授权认证的单钥算法、授权主密钥、对计算支付密码的公开钥签名算法确认和鉴别的指令、卡号、发行信息，

3、根据权利要求 2 所述的银行通用支付密码系统，其特征在于，所述支付密码卡中基本信息有：用于授权认证的单钥算法、计算支付密码的公开钥签名算法、验证签名的算法、授权认证子密钥、银行网点认证子密钥、用户口令子密钥、银行网点解锁密钥、支付密码秘密钥、人行清算中心公开钥信息、卡号、发行信息、客户基本信息，

4、根据权利要求 3 所述的银行通用支付密码系统，其特征在于，所述电子票据卡中的基本信息有：授权认证的单钥密码算法、授权认证子密钥、银行网点认证子密钥、用户口令密钥、银行网点口令解锁密钥、卡号、客户信息、票据文件、回执文件，

5、根据权利要求 4 所述的银行通用支付密码系统，其特征在于，所述证书管理的结构是，城市人行的证书管理工作站为银行网点和客户颁发证书，并保存所有的网点证书和客户证书，银行网点负责为自己和客户产生密钥对，并为自己和客户申请证书，网点保存本网点开户的客户证书、本网点证书和城市人行证书管理工作站的证书，客户带合法证明材料到网点开户，办理密钥生成和证书申请。

6、根据权利要求 5 所述的银行通用支付密码系统，其特征在于，所述证书的格式包括证书版本号、序列号、签名算法、证书签名、签发者、证书有效期、客户名称、开户行银行代码、帐号、公钥算法、公钥。

说　明　书

银行通用支付密码系统

银行支付密码系统，或称为银行电子交易系统，属于金融行业资金清算电子化技术领域。

目前，我国金融行业资金结算的主要方式之一为借记票据清算，借记票据支付的依据是钤印单位公章和法人代表名章。收款行须将原始票据提交付款行，由付款行进行人工核对，确认无误并付款后，收帐抵用。这种人工核对公章、名章的方式，不但不能实时处理借记票据，而且难辨图章真伪，经常导致资金被骗事件的发生。因而，近些年来，国内外开始研究和使用支付密码技术，在我国，各地使用的支付密码技术大致有四种模式，较有代表性的是①长沙模式：客户购买一台在银行注册后的支付密码座机，签发支票时将金额、日期等要素输入密码器，将产生的密码填写在支票上，银行以同样的方法计算，如相符，则支付。②青岛模式：客户先在银行预留企业法人、财会人员密码，购支票时，银行核对密码无误后，一次打印出相对应的整本支票的支付密码，客户在签发支票时，按银行打印好的密码清单填写对应的密码。③鞍山模式：客户预先在银行购买支付密码座机和票面下端贴有磁条的磁性支票，签发支票时，将支票在支付密码座机划槽划过，把信息记录在支票磁条上，收款方和银行通过密码器对支票进行校验。④东莞模式：采用 IC 卡方式，设主管卡、会计卡和采购员卡，卡内存有三者的密码，由卡证实其身份，从而间接确认票据的真实性和有效性。上述几种模式存在的问题是：1、采用单钥密码体制，即银行与客户共同使用同一密钥进行计算和检验，一旦出现问题，责任无法区分，2、密码核心部件与器具没有分离，密码算法存放在安全性较低的芯片中，且与机座无法分离，支付密码座机整机由厂方提供，银行与客户都不放心，3、标准不统一，技术不规范，各银行各自搞一套对公通兑系统，各行确定的密码器无法跨系统使用，使得各单位不得不在多家银行开户，并购买多个密码器，不利于财会人员操作又加重企业负担，4、没有设防伪密控部件，无法抵挡假冒伪劣产品混入和黑客入侵，5、适应性弱，在向“无纸化”、“电子支票”过渡时，该器具只能报废。

本发明旨在发明一种用于同城资金清算的通用支付密码系统，安全性高、适应性强、标准统一、技术规范，使用统一发行的 IC 卡、和按统一规范要求生产的支付密码座机，使各厂家的清算系统可构筑其上。

银行通用支付密码系统包括金融网络系统、清算软件系统、支付密码座机以及与支付密码座机配合使用的若干种 IC 卡，所述 IC 卡是授权认证卡、支付密码卡和电子票据卡，

授权认证卡是人总行配发的用于对支付者身份及支付行为的基本结算要素进行认证、并控制支付密码座机使用的 IC 卡，卡中基本信息有：用于授权认证的单钥算法、授权主密钥、对计算支付密码的公开钥签名算法确认和鉴别的指令、卡号、发行信息，

支付密码卡是客户用于为票据签字、并具有计算功能的 IC 卡，卡中的基本信息有：用于授权认证的单钥算法、计算支付密码的公开钥签名算法、验证签名的算法、授权认证子密

钥、银行网点认证子密钥、用户口令子密钥、银行网点解锁密钥、支付密码秘密钥、人行证书管理工作站公开钥信息、卡号、发行信息、客户基本信息，

电子票据卡是存放签发好的电子票据的 IC 卡，卡中的基本信息有：授权认证的单钥密码算法、授权认证子密钥、银行网点认证子密钥、用户口令密钥、银行网点口令解锁密钥、卡号、客户信息、票据文件、回执文件，

本系统包括以下几部分：

1）行业根密钥生成系统，由人民银行总行（以下简称人总行）内部指定专人秘密完成，下级密钥由上级密钥离散生成，

2）人总行的授权认证卡发行管理系统，包括安全服务、卡发行管理、卡档案管理三部分，它的安全服务模块调用密钥生成算法产生人行授权主密钥，把人行授权主密钥和支付密码卡卡号传给子密钥计算函数，产生支付密码卡认证子密钥，再把授权认证卡主密钥和电子票据卡卡号传给子密钥计算函数，产生电子票据卡认证子密钥，授权主密钥、认证子密钥采用单钥密码方案，它的卡发行管理模块调用卡号生成函数生成各种卡的卡号，并将授权认证卡、支付密码卡和电子票据卡分发给城市人行证书管理工作站。它的卡档案管理模块将卡分类管理，可查询统计发卡情况，识别卡的真伪、授权日期、有效期、使用地域等，

3）城市人行的证书管理系统，包括安全服务、证书管理、卡发行管理、和票据接收服务程序，它的安全服务模块采用公钥密码体制，RSA 密码方案，约定人总行、银行网点、客户只拥有一对自己的公钥公钥密钥对，公开钥用于验证签名，秘密钥用于签名。它的证书管理包括证书的申请、更新、挂失、复效、重发及查询、统计等辅助功能，它的卡发行管理对卡进行应用初始化，即建立应用卡结构、写应用基本信息，并进行卡档案管理，它的票据接收服务程序负责处理客户开具的电子票据从支付密码座机拨号到城市人行清算中心的接收工作，

4）银行网点的证书管理系统，包括安全服务、证书管理和票据接收，它的安全服务模块，其算法由一块插在计算机中的硬件加密卡实现，它内置 RSA 密码技术，产生网点及客户的公钥密钥对，对通讯包加密/解密，对证书申请信息和清算信息进行签字/验证，它的证书管理包括证书的申请、更新、挂失、复效、重发及查询、统计等辅助功能，它的票据接收包括支付密码座机和票据接收程序，支付密码座机带有授权认证卡，与电子票据卡互相认证，校验电子票据卡口令，选取票据，处理票据接收程序返回的清算结果回执，

5）客户的支付密码座机系统，包括支付密码座机、支付密码卡和电子票据卡，它的支付密码座机是配合授权认证卡使用、用于签发和验收电子票据卡的终端设备。

使用本系统进行交易的基本过程是这样的，系统涉及三种 IC 卡，即起认证作用的授权认证卡、相当于数字签名的支付密码卡、相当于电子支票的电子票据卡，首先，在人总行授权认证中心生成三种卡的授权主密钥、认证子密钥并产生卡号，客户通过人总行的卡发行系统取得三种卡后，使用时，先将授权认证卡插入其购买的支付密码座机，得到认证后（未经认证的支付密码座机不允许在系统中使用），在支付密码座机上对支付密码卡和电子票据卡写入数据，并通过支付密码座机与城市人行的清算中心结算，或者通过银行网点与城市人行清算中心结算。由于支付密码座机在插入授权认证卡后才可使用，授权认证卡又是由银行发

放的，因此，可以有效防伪。专门研制的支付密码座机，其核心部件支付密码卡、电子支票卡与支付密码座机插接，可以分离，生产厂商只提供支付密码座机裸机，提高了安全性。系统采用单钥、公钥并用，单钥用于人总行授权认证，规范厂商行为，加强行业管理；公钥体制用于验证数字签名，即解决信息的安全认证问题，每个客户对应一对公钥密钥对——公开钥和秘密钥，银行只掌握公开钥，客户掌握秘密钥。一旦出现泄密，容易分清各自的法律责任。使用本系统，有效地加快了资金清算，并解决了票据的安全性问题，可顺利实现向“无纸化”和“电子支票”系统的过渡。

图 1　银行通用支付密码系统示意图

图 2　银行通用支付密码系统功能框图

图 3　认证子密钥左半部的推导方法

图 4　认证子密钥右半部的推导方法

图 5　客户证书申请过程示意图

图 6　票据接收服务程序与支付密码座机的关系示意图

图 7　授权认证卡认证过程示意图

图 8 票据签发过程示意图

图 9 票据验收过程示意图

下面结合附图说明本发明的最佳实施例。参见图 1，金融网络系统已由各地人行建立，清算软件系统已开发并投入运行，涂黑部分为本支付密码系统提供的新功能。

人总行授权认证卡发行管理系统，参见图 2，

1）安全服务模块产生一个授权主密钥，在人总行决定的一定使用期内，授权主密钥是唯一的，只能产生一次；

2）为授权认证卡生成专用唯一的卡号，登记备案，并通过 IC 卡读写器把授权主密钥和卡号写入授权认证卡，将授权认证卡分发给城市人行证书管理工作站；

3）为支付密码卡生成专用唯一的卡号，登记备案，并由安全模块根据授权主密钥和卡号计算生成认证子密钥，把子密钥和卡号一起通过 IC 卡读写器写入支付密码卡；

4）为电子票据卡生成专用唯一的卡号，登记备案，并由安全模块根据授权主密钥和卡号计算生成认证子密钥，把子密钥和卡号一起通过 IC 卡读写器写入电子票据卡；

5）把已生成（授权认证）的支付密码卡和电子票据卡分发到城市人行证书管理工作站。

上述用于授权和认证的密码算法采用国家密码委批准的、中国人民银行保密办认可的单钥密码算法。授权主密钥和认证子密钥使用 16 字节密钥。授权主密钥由人总行秘密产生，认证子密钥由授权主密钥与客户卡卡号推导生成。推导方法参见图 3 和图 4。

城市人行证书管理系统如图 2 所示，由安全服务、证书管理、卡发行管理和票据接收服务四部分组成。

一、安全服务　安全服务采用 RSA 密码方案，约定每个实体（即城市人行证书管理工作站、银行网点、客户）只拥有一对自己的密钥，公开钥用于验证签名，秘密钥用于签名，RSA 采用 1024 位模长。

签名过程如下：

1、 将原文（本系统为签名要素）通过算法压缩为 20 字节的消息摘要，如果原文长度小于 20 字节，在原文后补 0，使原文达到 20 字节，然后再通过算法压缩为 20 字节的消息摘要；

2、 用秘密钥通过签名算法对消息摘要进行签名运算，得到签名，签名长度为 1024 位

3、 将原文和签名传递给接收者

验证过程如下：

1、 将收到的原文通过算法压缩为 20 字节的消息摘要，如果原文长度小于 20 字节，在原文后补 0，是原文达到 20 字节，然后在通过算法压缩为 20 字节的消息摘要，

2、 按发文方标识从证书库取出发文方公钥；

3、 将发文方公钥、消息摘要和签名一并作为输入送给签名验证算法进行验证；

4、 验证通过，说明收文确实来自发文方，如果未通过验证，则说明收文系伪造或在传送过程中受损。

本系统的签名/验证用于以下过程：

1、 客户证书申请和管理过程

2、 票据签验过程

3、 票据清算信息传送过程。

安全服务器是一台物理计算机，是 RSA 密码技术的硬件实现，负责公钥密钥对的产生和存储，清算信息的签名和验证也在这里运算，它通过一套安全接口函数供清算软件和证书管理调用以实现安全功能。安全服务器与清算服务器之间以高速网络方式互连，以解决网络通讯的瓶颈问题，提高系统的整体性能。

二、证书管理系统　证书管理系统为银行网点和客户签发证书，并负责证书的管理工作，本系统只设一个证书管理工作站，即城市人行证书管理工作站，证书管理工作站的证书由自己产生并签发，并通过法律公证或公开登报等方式加以确认。证书管理系统包括证书管理结构、证书管理功能、证书格式三部分。

（一）证书管理结构如下：

城市人行证书管理工作站（CA）：CA 由城市人行设立并维护，负责为银行网点和客户颁发证书，并把 CA 的证书分发给网点，CA 保存所有的网点证书和客户证书。

银行网点：负责为自己和客户产生公钥密钥对，并为自己和客户申请证书，网点只保存在本网点开户的客户证书、本网点证书以及 CA 的证书。

客户：客户必须拥有银行网点的合法帐户或携带合法证明材料到网点开户，携带合法证明材料到网点办理密钥生成和证书申请。

（二）证书管理功能如图 2 所示，

证书签发用于本系统首次使用时各种证书的签发和新开户客户证书的签发 。在本系统中，所有证书的签发都由城市人行证书管理工作站（CA）签发，证书的签发方式有人工传送和网络传送两种。如图 5 所示，客户证书的签发过程如下：

1、 携带合法证明材料到开户的商业银行网点

2、 网点验证客户提供的证明材料

3、 网点通过安全服务模块为客户产生公钥密钥对

4、 网点用客户公钥及客户信息形成证书申请书，签字后，通过银行网络发送给 CA；

5、 CA 接收并验证客户证书申请书，检查客户帐户的有效性，同时把该客户证书保存在 CA 的客户证书库中；

6、 网点收到客户证书并验证后，将客户证书存入本地证书库。

7、 网点把客户秘密钥、CA 的证书以及其它信息立即写入客户的支付密码卡，交客户带回，网点不留客户的支付密码。

网点证书的签发过程如下：

1、 网点通过安全服务模块产生网点的公钥密钥对

2、 将网点密钥保存在安全地方（如加密卡中）；

3、 网点派专人、或通过网络将本网点公钥及相关证书申请材料送到城市人行证书管理工作站 CA；

4、 CA 验证网点的合法性；

5、 CA 为网点产生网点证书，签字后把证书、CA 的证书一起交给网点所派专人带回，或通过网络发出通知，同时将网点证书存入 CA 证书库；

6、 网点得到 CA 证书后，将本网点的证书、CA 的证书存入本网点的证书库。

CA 证书由自己签发，过程如下：

1、 CA 通过安全服务器产生一对公钥对；；

2、 CA 将秘密钥保存在安全服务器中；

3、 CA 为自己产生证书，用自己的秘密钥为证书签字 ，把 CA 的证书存入 CA 的证书库

4、 城市人行证书管理工作站将 CA 证书通过法律公证或公开登报等方式加以确认。

证书更新 所有证书应定期更新，更新的周期由城市人行决定，其过程与签发过程相似。

证书挂失 证书挂失指客户证书的挂失，由客户到开户银行网点受理，过程如下：

1、 客户携带有效证明材料，到客户开户银行网点，

2、 网点验证客户提供的证明材料，

3、 网点生成客户证书挂失申请书，签字后通过银行网络发送给 CA，

4、 CA 接受并验证客户证书挂失申请书，形成证书挂失批准回执，签字后发给网点，同时写入 CA 的挂失证书库，修改 CA 证书库中该证书的状态为挂失状态；

5、 网点接收并验证回执，写入本地挂失证书库，修改本地证书库中该证书的状态为挂失状态；

6、 网点给客户开具证书挂失证明，交客户带回。

证书复效 指客户证书的复效，复效由客户支付密码卡找回等原因引起，证书复效必须在证书挂失有效期内办理，逾期必须申请证书重发。过程如下：

1、 客户携带银行网点开具的证书挂失证明和有效证明材料到客户开户银行网点；

2、 网点验证客户提供的证明材料；

3、 网点生成客户证书复效申请书，签字后通过银行网络发送给 CA；

4、 CA 接收并验证客户证书复效申请书，形成证书复效批准回执，签字后发给网点，同时写入 CA 的修改挂失证书库，重置 CA 证书库中该证书的状态为有效状态；

5、 网点接收并验证回执，修改本地挂失证书库，重置本地证书库中该证书的状态为有效状态；

6、 网点给客户收回证书挂失证明，通知客户已复效。

证书重发 指客户证书的重发，过程如下：

1、 客户携带银行网点开具的证书挂失证明和有效证明材料到客户开户银行网点；

2、 网点验证客户提供的证明材料；

3、 网点查询挂失证书库，核实该客户证书已挂失；

4、 网点通过安全模块为客户产生公钥密钥对；

5、 网点把客户秘密钥、CA 的证书及其它信息立即写入客户的支付密码卡交客户；

6、 网点生成客户证书重发申请书，签字后通过银行网络发送给 CA；

7、 CA 接收并验证客户证书重发申请书，产生新的客户证书，签字后发给申请网点，同时，CA 修改挂失证书库，将该客户的旧证书转入失效证书库，将新证书写入 CA 证书库；

8、 网点接收并验证客户证书，修改本地挂失证书库，将旧的客户证书转入失效证书库，将新的客户证书存入本地证书库；

9、 网点给客户收回证书挂失证明，通知客户已重发。

辅助功能 包括各类证书的查询、统计等工作

（三）证书格式

名称	描　　述
版本	证书版本号
序列号	CA 赋予证书的唯一序列号
签名算法	定义用于签名的算法
签名	证书签名
签发者	CA 的名称
有效期	证书有效期（起始日期）
有效期	证书有效期（终止日期）
单位名称	客户名称
开户行	客户的开户银行代码
帐号	客户的银行帐号
公钥算法	说明公钥使用的算法
公钥	公钥内容

三、卡发行管理　首先是应用初始化　城市人行证书管理工作站从人总行领回支付密码卡和电子支票卡后，对支付密码卡和电子票据卡进行应用初始化工作，建立应用卡结构，写应用基本信息等，完成后，由各银行网点领走，进行最终发行。

三、票据接收服务程序　客户开具的电子票据可以从支付密码座机通过 PSTN 拨号到城市清算中心，由清算中心的票据接收服务程序接收并提交清算，票据接收服务器与支付密码座机的关系如图 6 所示。票据接收服务程序的处理过程描述：

1、 从通讯端口接收支付密码座机传来的票据；
2、 向支付密码座机发送票据已接收信息；
3、 以票据的帐号和票据号为键值查询票据清算状态库；
4、 如果存在信息，说明本张票据已提交清算过，提取信息，形成回执，签字后发给支付密码座机，并断开通讯连接；
5、 如果不存在信息，说明是首次提交的票据；
6、 把票据提交给清算软件，由清算软件进行票据清算；
7、 循环查询清算中心的票据清算状态库；
8、 从清算状态库提取清算结果信息；
9、 将清算结果信息形成回执，用清算中心密钥签字；
10、 将带清算中心签字的回执发送给处于等待状态的支付密码座机；
11、 断开与支付密码座机之间的通讯连接。

银行网点的证书管理系统，如图 2 所示，包括安全服务和票据接收。

一、安全服务 在银行网点系统中，由于安全算法、证书管理、卡发行管理等三项工作密切相关，所以集中在安全服务模块来管理。银行网点的安全算法由一块插在计算机中的硬件加密卡来实现，它内置 RSA 密码技术，在软件上提供一套安全接口函数供调用，安全接口函数与清算中心的安全服务器提供的接口函数相同，作用如下：

1、 产生网点及客户的公钥密钥对；
2、 通讯包的加密/解密；
3、 证书申请信息的签字/验证；
4、 清算信息的签字/验证；

证书管理　网点的证书管理与清算中心的证书管理协同工作，完成证书的申请、签发、更新、挂失、复效、重发等工作。

卡发行管理　客户卡由网点从城市人行证书管理工作站领回，客户卡分支付密码卡和电子支票卡两种，每个客户必须有一张支付密码卡和一张或几张电子票据卡。

卡客户化　卡发行的最终形式是卡的客户化工作，由网点在客户申请证书时完成，过程如下：

1、 客户持有效证明材料到开户行申请客户证书；
2、 网点验证客户提供的证明材料；
3、 网点为客户生成支付密码，并向 CA 申请证书；

4、 网点对支付密码卡和电子票据卡做客户化工作，如写入客户和银行基本信息等，并可由客户现场设置口令；

5、 网点把支付密码、CA 证书写入支付密码卡；

6、 将支付密码卡和电子票据卡交给客户带回。

二、票据接收　客户用支付密码座机签发的票据均存在电子票据卡中，持卡购物时，卖方可能不具备通过支付密码座机联机清算的能力，可到银行网点办理支付。网点配备票据接收系统处理此类需求。

网点的票据接收系统由支付密码座机和票据接收程序组成。

支付密码座机处理过程如下；

1、 等待插入电子票据卡；

2、 与电子票据卡互相认证；

3、 验证电子票据卡口令；

4、 选取用于本次支付的票据；

5、 将票据数据发送给票据接收程序；

6、 等待票据接收程序的清算结果；

7、 接到回执后，在电子票据卡中记录回执；

8、 修改选定票据的状态，退出。

票据接收程序的处理过程如下：

1、 等待支付密码座机发送数据；

2、 读取支付密码座机发来的票据；

3、 把票据提交给网点的清算服务程序；

4、 循环查询网点的票据清算状态库；

5、 从票据清算状态库提取清算结果；

6、 将清算结果形成回执发送给处于等待状态的支付密码座机；

7、 回到等待状态。

客户的支付密码座机系统　如图 2，客户系统由支付密码座机系统、支付密码卡和电子票据卡组成。每个客户必须拥有一张支付密码卡和至少一张电子票据卡，但不一定拥有支付密码座机。没有支付密码座机的客户可以携带自己的支付密码卡和电子票据卡到拥有支付密码座机的客户那里去签验票据，也可直接到网点，使用网点的支付密码座机签验票据。支付密码座机是一个带有授权认证卡的通用设备，任何客户都可以用它进行电子票据的签发和验收，签发和验收分联机和脱机两种模式。

联机模式　客户使用支付密码座机将签发或验收的票据直接通过电话拨号发送给清算中心的票据接收服务程序，由票据接收服务程序直接提交清算，支付密码座机等待清算中心的清算结果回执，验证并将回执记录在电子票据卡中，联机方式可以视为由客户直接发起票据清算。

脱机模式　签发票据时，客户使用支付密码座机将签发的票据存入电子票据卡中，携电

子票据卡外出购物或到网点办理支付，验收票据时，如果收款方没有支付密码座机，收款方可与付款方一起到网点办理支付，如果收款方有支付密码座机，收款方通过支付密码座机验收付款方的票据，并将验收的票据写入收款方的电子票据卡中，事后到网点办理支付或通过支付密码座机提交清算。

支付密码座机的组成包括存储器、显示部件、IC 卡读写接口、调制解调器、打印模块、键盘，配合授权认证卡、支付密码卡和电子票据卡的使用，具有授权认证、票据签发、票据验收、票据查询、票据提交、辅助管理等功能。

授权认证　指支付密码座机中的授权认证卡与客户支付密码卡和电子票据卡之间的认证，作用是保证客户使用的支付密码卡和电子票据卡一定是经人总行授权发行的卡，只有认证通过后，才能进行其它处理，认证过程如图 7 所示，授权认证卡中存有授权主密钥，每张客户卡（支付密码卡、电子票据卡）上都存有由授权主密钥根据卡号计算的授权认证子密钥，由于卡号唯一，每张卡上的认证子密钥都是不一样的，因此，每次认证时，授权认证卡现场根据卡号计算工作密钥（即授权认证子密钥）后再与卡认证，这样，每张卡的认证过程使用的是不同的认证密钥，从而有效地保护卡中密钥的安全。

票据签发　票据签发人必须持有支付密码卡，以对票据进行签名。在签发过程中，每次插卡都要经过例行的认证过程，认证通过后方可继续。票据的种类有多种，如：转帐支票、限额支票、现金支票等，票据的录入过程应是一个可定义的过程，支持各地票据种类和票据内容。在验证支付密码卡和电子票据卡口令时，只允许连续输错三次，超过三次卡自动锁死，不允许再试，必须到网点进行解锁，其它处理过程中验证卡口令的处理情况相同。票据签发的基本过程如图 8 所示。

票据验收　收款方收到付款方的电子票据后，可直接通过支付密码座机验收并提交给清算中心清算，也可以通过支付密码座机将付款方电子票据卡中用于支付本笔款项的电子票据检验后转入自己的电子票据卡中。基本过程如图 9 所示。

票据查询　用于在支付密码座机上查询自己电子票据卡中的所有票据（包括自己签发和验收付款方的票据）；票据查询处理过程如下：

1、 在支付密码座机中插入电子票据卡；

2、 支付密码座机认证电子票据卡；

3、 支付密码座机验证电子票据卡口令；

4、 列出电子票据卡中所有票据的票据号；

5、 客户选取票据号；

6、 支付密码座机提取客户选取的票据内容供客户浏览；；

7、 浏览完毕后，退出。

票据提交　用于通过支付密码座机提交未清算的票据，未清算的票据包括在票据签发或验收中未当时通过电话拨号方式向清算中心提交的票据，以及虽然已向清算中心提交，但由于通讯线路故障或其它原因未收到清算中心回执的票据。对于第一种情况，处理过程如下：

1、 在支付密码座机中插入电子票据卡；

2、 支付密码座机认证电子票据卡；
3、 支付密码座机验证电子票据卡口令；
4、 列出电子票据卡中未清算票据的票据号；
5、 客户选取票据号；
6、 支付密码座机提取客户选取的票据内容供客户浏览；
7、 支付密码座机提示客户确认提交清算；
8、 支付密码座机通过电话拨号与清算中心建立通讯连接；
9、 将客户选定的票据发送给清算中心；
10、 等待清算中心的回执；
11、 验证清算中心的回执；
12、 在电子票据卡中记录回执。
13、 退出

对于第二种情况的票据提交，处理过程与第一种情况的处理过程完全一样，只是清算中心的处理有区别。清算中心接收到票据后，首先以帐号和支票号为唯一键值检索清算状态库，如果存在信息，则提出信息形成回执，签字后发给支付密码座机，如果没有信息，则按正常提交程序进行清算。

辅助管理 包括更改支付密码卡口令、更改电子票据卡口令、支付密码座机日期设置、清算中心电话号码设置、票据整理等，更改支付密码卡口令的过程如下：

1、 在支付密码座机中插入支付密码卡；
2、 支付密码座机认证支付密码卡；
3、 支付密码座机验证支付密码卡口令；
4、 双遍输入新口令；
5、 核对两遍输入的内容是否一致；
6、 不一致，更改失败，退出；
7、 一致，向支付密码卡发口令更改指令；
8、 正确返回，退出。

更改电子票据卡口令的过程如下：

1、 在支付密码座机中插入电子票据卡；
2、 支付密码座机认证电子票据卡；
3、 支付密码座机验证电子票据卡口令；
4、 核对两遍输入的内容是否一致；
5、 不一致，更改失败，退出；
6、 一致，向电子票据卡发口令更新指令；
7、 正确返回，退出。

本系统适用于所有需在全国或国内一定地域进行统一认证管理的业务及其管理部门，例如，汇票防伪安全管理、全国证券业务管理，财税、电力、海关、邮电、公安等部门。

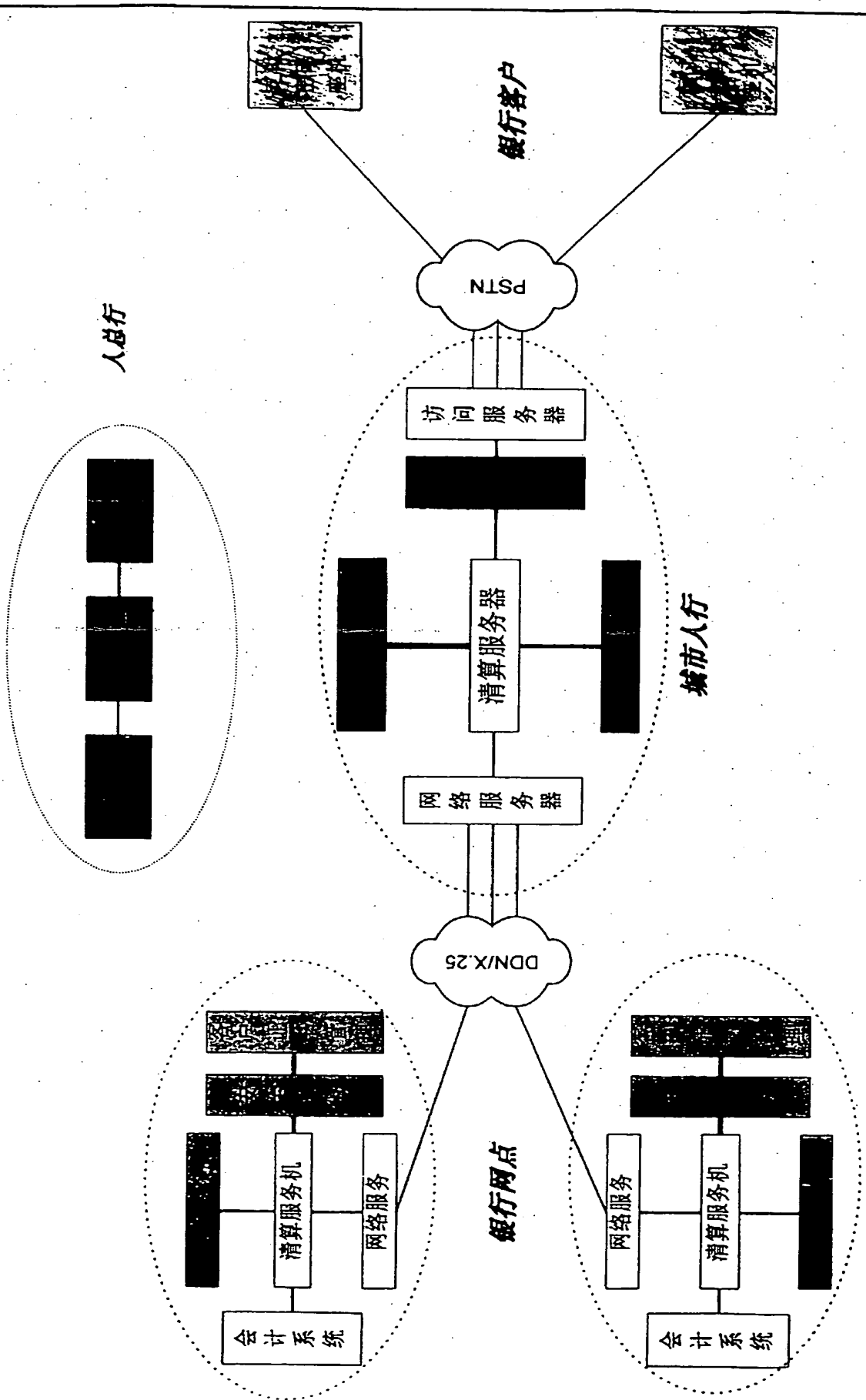


图 1

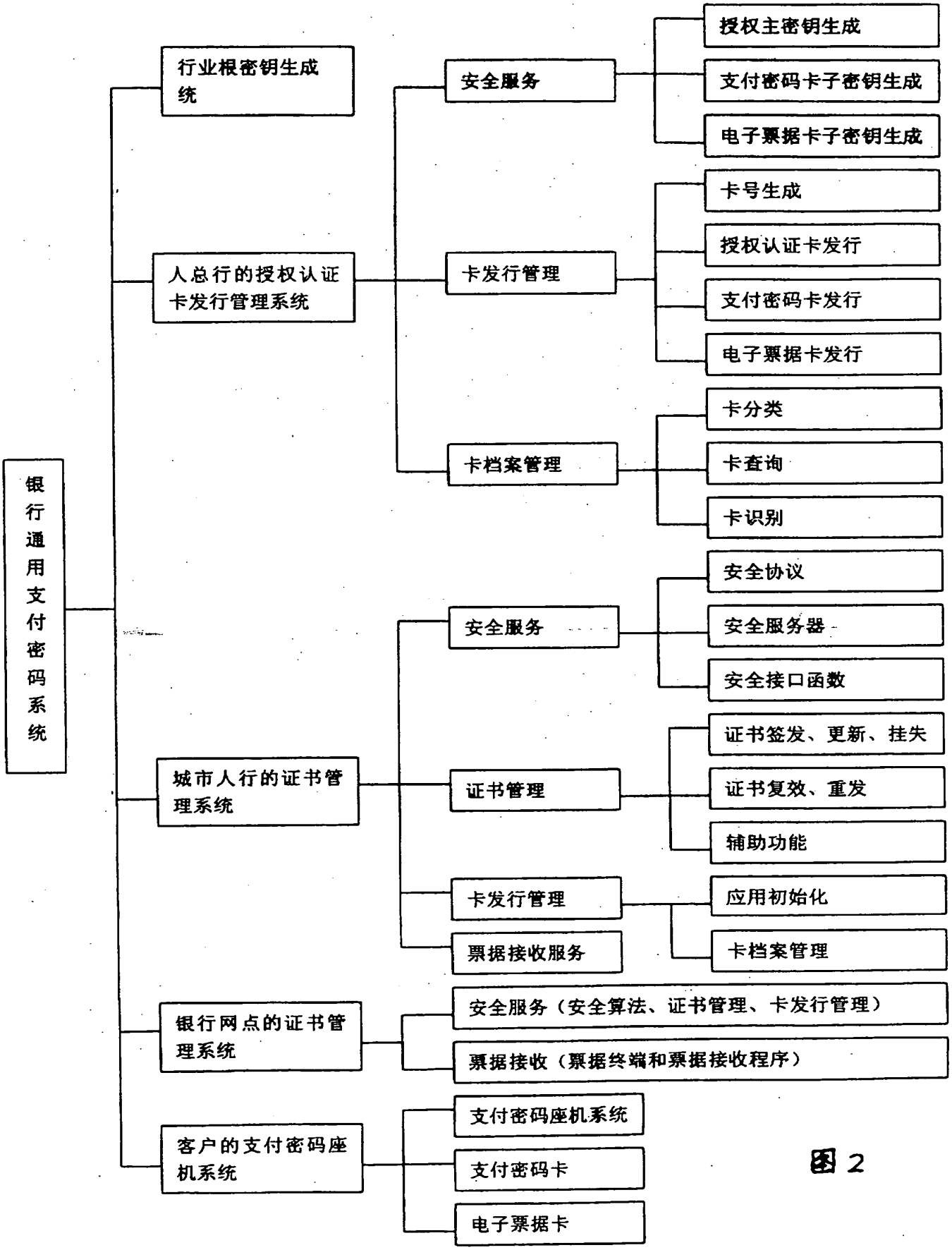


图 2

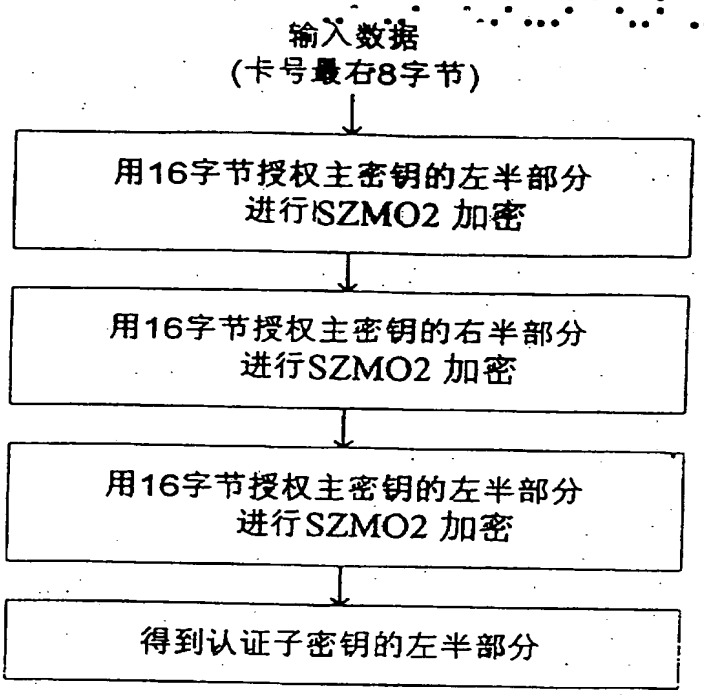

输入数据
(卡号最右8字节)
用16字节授权主密钥的左半部分
进行SZMO2 加密
用16字节授权主密钥的右半部分
进行SZMO2 加密
用16字节授权主密钥的左半部分
进行SZMO2 加密
得到认证子密钥的左半部分

图 3

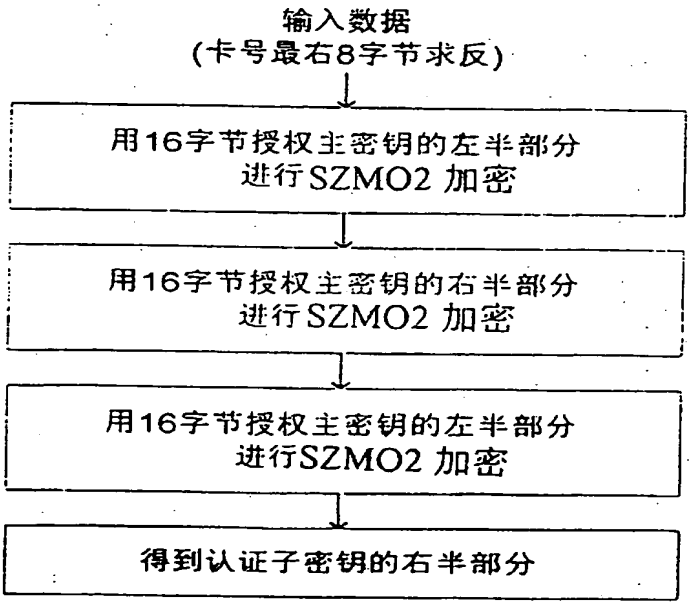

输入数据
(卡号最右8字节求反)
用16字节授权主密钥的左半部分
进行SZMO2 加密
用16字节授权主密钥的右半部分
进行SZMO2 加密
用16字节授权主密钥的左半部分
进行SZMO2 加密
得到认证子密钥的右半部分

图 4

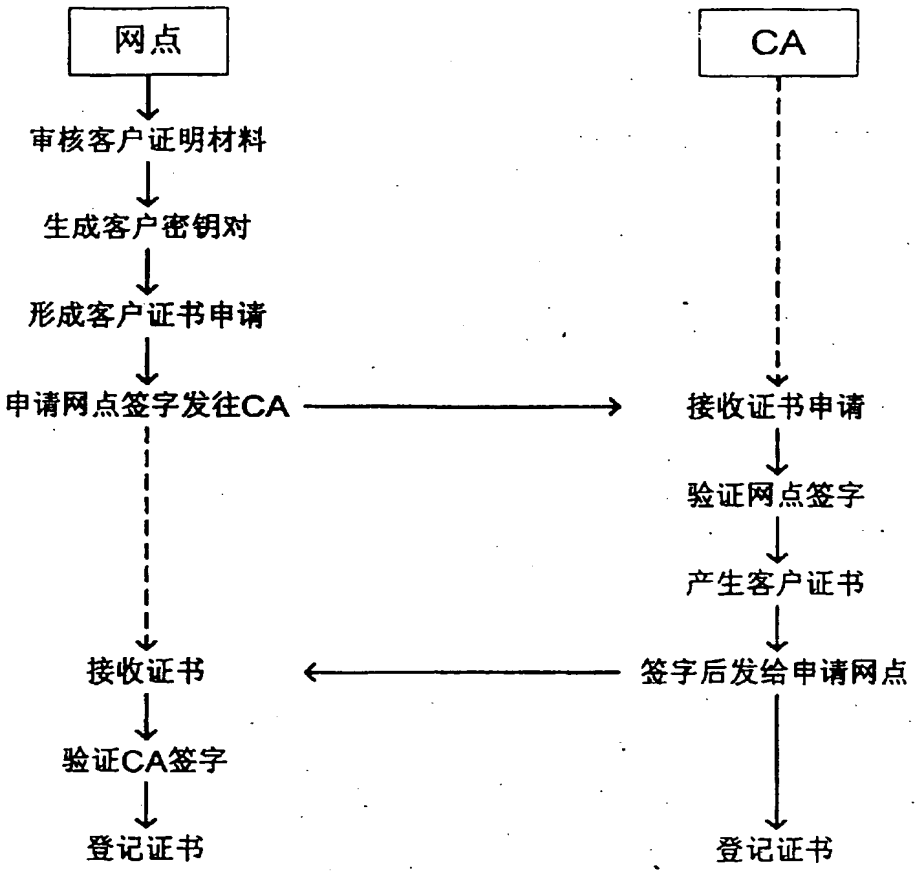

网点
CA
审核客户证明材料
生成客户密钥对
形成客户证书申请
申请网点签字发往CA
接收证书申请
验证网点签字
产生客户证书
接收证书
签字后发给申请网点
验证CA签字
登记证书
登记证书

图 5

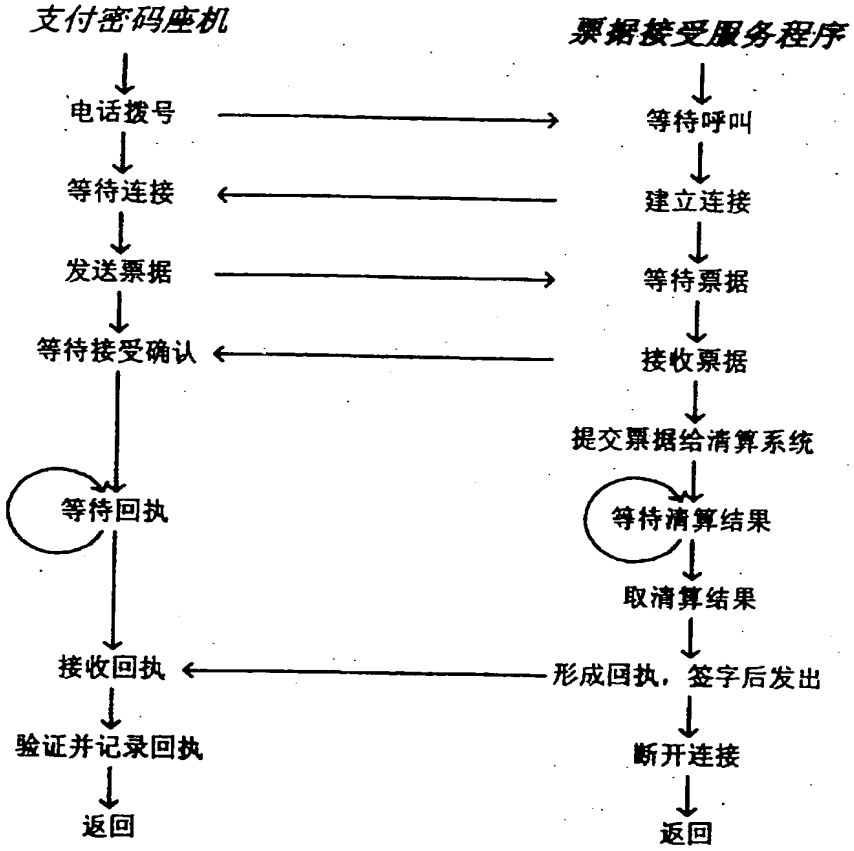

支付密码座机
票据接受服务程序
电话拨号
等待呼叫
等待连接
建立连接
发送票据
等待票据
等待接受确认
接收票据
提交票据给清算系统
等待回执
等待清算结果
取清算结果
接收回执
形成回执，签字后发出
验证并记录回执
断开连接
返回
返回

图 6

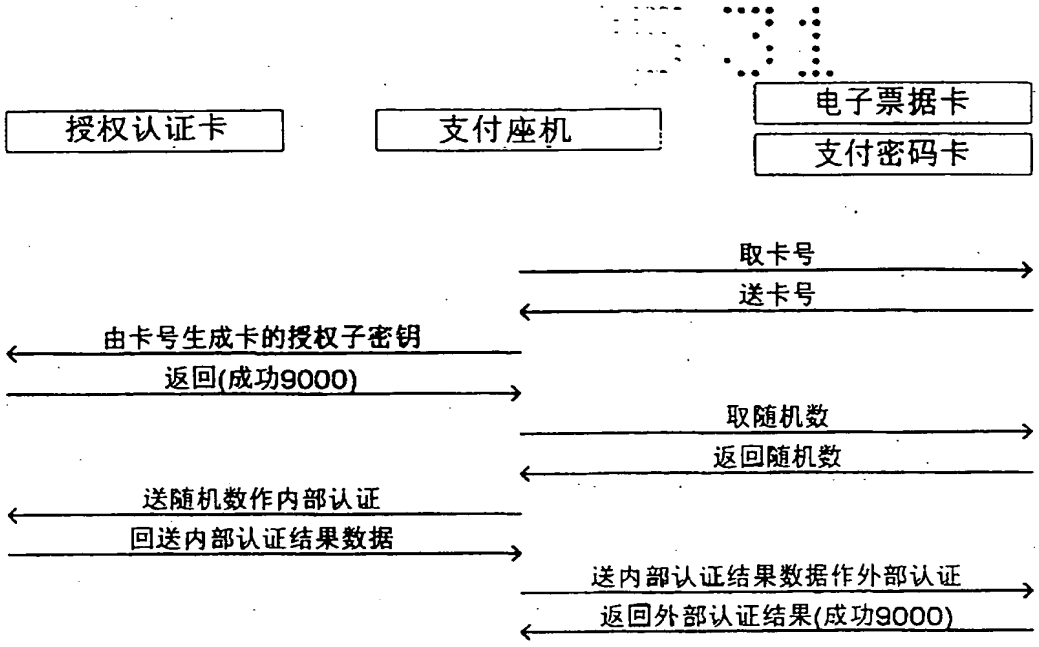

授权认证卡
支付座机
电子票据卡
支付密码卡
取卡号
送卡号
由卡号生成卡的授权子密钥
返回(成功9000)
取随机数
返回随机数
送随机数作内部认证
回送内部认证结果数据
送内部认证结果数据作外部认证
返回外部认证结果(成功9000)

图 7

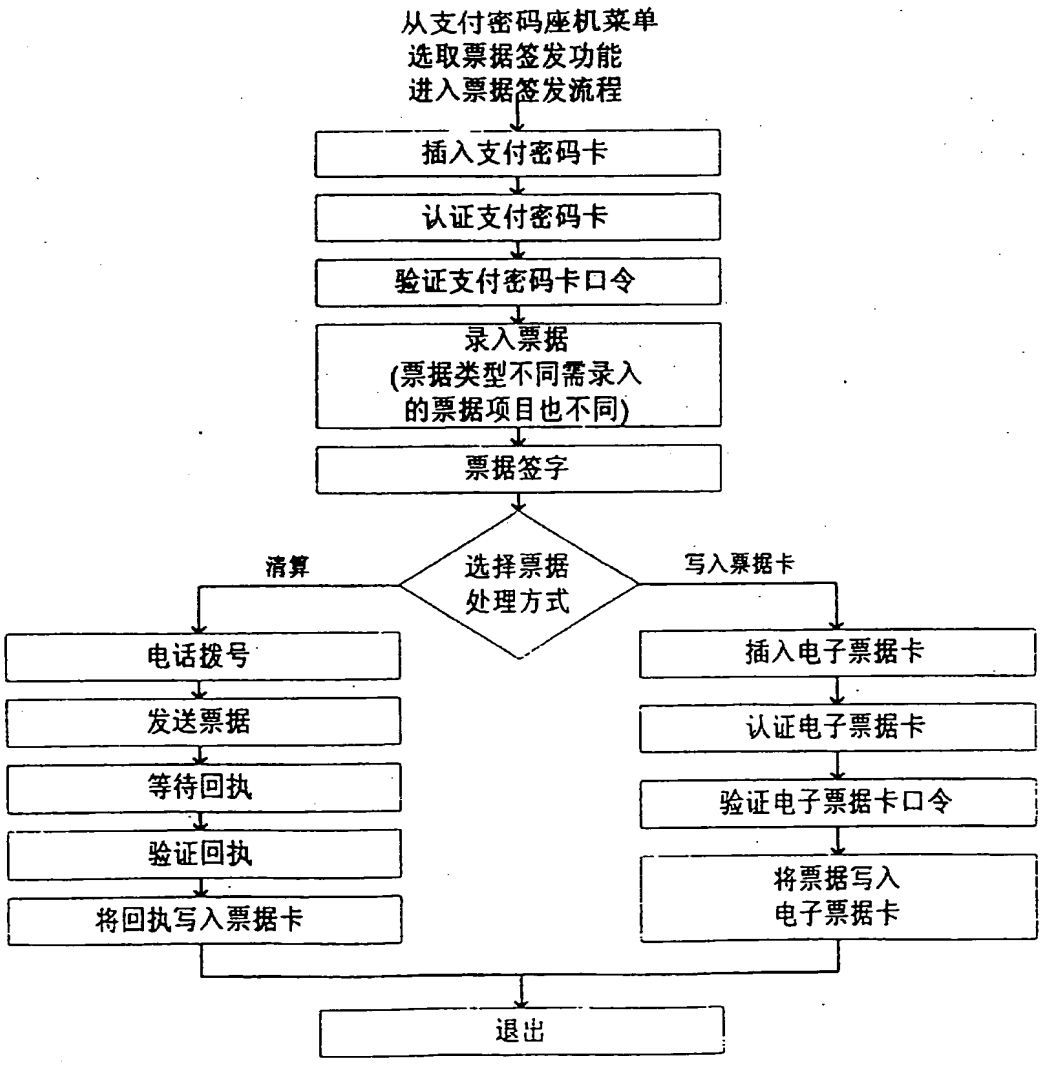

从支付密码座机菜单
选取票据签发功能
进入票据签发流程
插入支付密码卡
认证支付密码卡
验证支付密码卡口令
录入票据
(票据类型不同需录入
的票据项目也不同)
票据签字
选择票据
处理方式
清算
写入票据卡
电话拨号
发送票据
等待回执
验证回执
将回执写入票据卡
插入电子票据卡
认证电子票据卡
验证电子票据卡口令
将票据写入
电子票据卡
退出

图 8

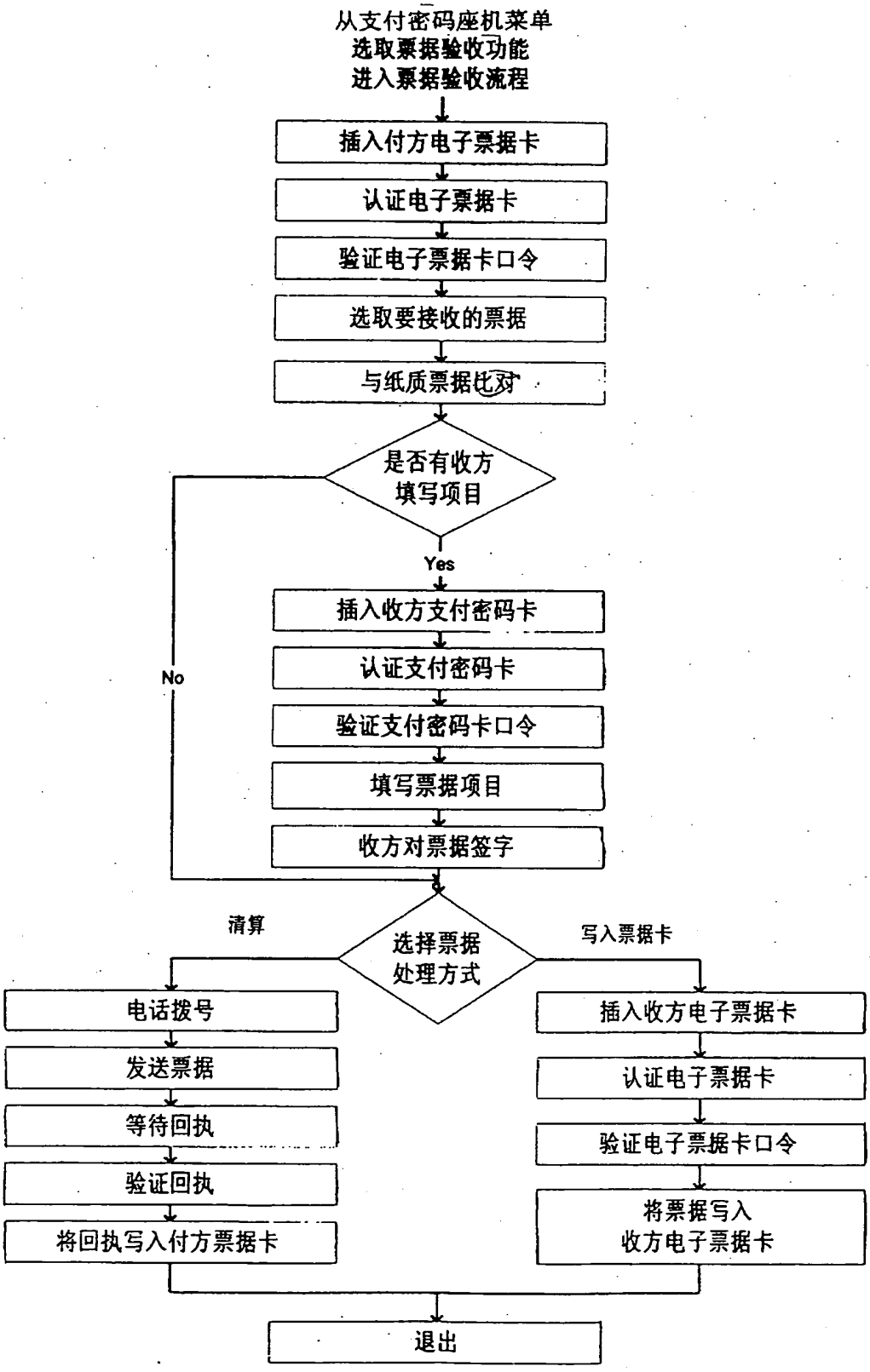

从支付密码座机菜单
选取票据验收功能
进入票据验收流程
插入付方电子票据卡
认证电子票据卡
验证电子票据卡口令
选取要接收的票据
与纸质票据比对
是否有收方
填写项目
Yes
No
插入收方支付密码卡
认证支付密码卡
验证支付密码卡口令
填写票据项目
收方对票据签字
选择票据
处理方式
清算
写入票据卡
电话拨号
发送票据
等待回执
验证回执
将回执写入付方票据卡
插入收方电子票据卡
认证电子票据卡
验证电子票据卡口令
将票据写入
收方电子票据卡
退出

图 9